

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE**

**K.L., on behalf of herself and all others
similarly situated,**

Plaintiffs,

vs.

PSYCH CARE CONSULTANTS, L.L.C.,

Serve registered agent:
Joanna Owen
763 S. New Ballas Road, Ste. 300
St. Louis, MO 63141

and QRS, INC.,

Serve registered agent at:
2010 Castaic Lane
Knoxville, Tennessee 37932

Defendants.

Case No. _____

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

COMES NOW Plaintiff K.L., on behalf of herself and all others similarly situated (together, “Plaintiffs”), by and through their undersigned attorneys of record, for their Petition against Defendants Psych Care Consultants, L.L.C. (“PCC”) and QRS, Inc. (“QRS”), and state to the Court as follows:

1. This is a class action on behalf of the thousands of patients whose sensitive health and personal information, including psychiatric diagnostic and treatment information, that was entrusted to PCC and QRS was compromised, accessed, and disclosed to one or more bad actors. This unauthorized access and disclosure occurred over at least three days and is believed to have been discovered on August 26, 2021 (“Protected Information Security Failure”). Yet, Plaintiff was

not notified of this event for three months when a letter was finally sent to her on or about November 26, 2021.

2. The Protected Information Security Failure occurred when one or more unknown hackers accessed the system run by PCC's patient portal vendor, QRS, Inc.

3. The information compromised during the Protected Information Security Failure includes, but is not limited to: names, Social Security Numbers, dates of birth, patient numbers, portal usernames, addresses, treatment, and diagnostic information.

4. Since PCC's patients were notified on November 26, 2021, acknowledged ransomware threat actors claimed responsibility for the Protected Information Security Failure on their dedicated information leak site or about November 30, 2021.

5. Plaintiff brings this class action because Defendants failed in their basic, legally-bound, and expressly-promised obligation to secure and safeguard PCC's patients' protected health information ("PHI"), as that term is defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and personally identifiable information ("PII") (collectively, "Protected Information").

6. Both Defendants are covered by HIPAA (45 C.F.R. § 160.102). As such, they are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

7. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

8. HIPAA requires Defendant to “comply with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

9. Defendants were also prohibited by the Federal Trade Commission Act (“FTCA”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (the “FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTCA. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

10. In addition to the above duties imposed by statute and regulation, Defendants owed a duty to Plaintiffs, to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Protected Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs, to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected Plaintiffs’ Protected Information.

11. As a result of PCC and QRS’s failure to secure the Protected Information it was entrusted with, and legally obligated—to safeguard, Plaintiffs’ sensitive medical and psychiatric information has been exposed. And Plaintiffs have suffered a loss of value of their Protected Information and have been exposed to and/or are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future.

12. PCC and QRS could have prevented this theft had it limited the patient information it shared and employed reasonable measures to ensure their business associates implemented and

maintained adequate data security measures and protocols in order to secure and protect PCC's patients' data.

13. During the Protected Information Security Failure, PCC and QRS maintained their medical record systems in a condition vulnerable to unknown, unsupervised, and unauthorized access by people with neither the required right of nor the need to access those records. This resulted in the improper access and disclosure of Plaintiffs' Protected Information. Upon information and belief, the mechanisms of the unauthorized disclosures of Plaintiffs' Protected Information were known risks to PCC and QRS, and, thus, PCC and QRS were on notice that failing to take steps necessary to secure their medical record systems from those risks left that property in a dangerous condition.

14. PCC and QRS failed to properly safeguard Plaintiffs' Protected Information, allowing unauthorized access to their Protected Information. PCC also failed to properly monitor the systems of their vendors. Had PCC properly monitored their vendors, PCC could have prevented the unauthorized access and disclosure or would have discovered the unauthorized access and disclosure sooner.

15. Armed with the information accessed in the Protected Information Security Failure, information thieves can commit a variety of bad acts including that adversely impact Plaintiffs, *e.g.* blackmail or extortion by those who threaten to further disclose the highly sensitive information breached unless the affected individuals pay a ransom, opening new financial accounts in their names, taking out loans in their names, using these names to obtain medical services, using their health information to target other phishing and hacking intrusions based on their individual health needs, using their information to obtain government benefits, filing fraudulent tax returns using Plaintiffs' information, among other malfeasance.

16. Because of the Protected Information Security Failure, Plaintiffs no longer have autonomy and control over their medical and treatment histories. They have no idea who may now have access to this information.

17. As a further consequence of the Protected Information Security Failure, Plaintiffs have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs must now and in the future closely monitor their financial accounts to guard against identity theft.

18. Plaintiffs may also incur out of pocket costs for, *e.g.* purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

19. Plaintiff K.L. seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Protected Information was compromised, accessed, and disclosed during the Protected Information Security Failure.

20. Plaintiff seeks remedies including, but not limited to: compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to PCC's and QRS's medical records security systems, future annual audits, and adequate credit monitoring services funded by PCC and QRS.

21. PCC's and QRS's intentional, willful, reckless, and/or negligent conduct—failing to prevent the Protected Information Security Failure, failing to limit their severity, failing to detect it in a timely fashion, and failing to timely notify Plaintiffs—damaged Plaintiffs uniformly. For this reason, PCC and QRS should pay for appropriate identity-theft protection services and reimburse Plaintiffs for the costs of PCC's and QRS's sub-standard security practices and failure to timely disclose the Protected Information Security Failure. Plaintiffs are, therefore, entitled to injunctive and other equitable relief that safeguards their information, requires PCC and QRS to

significantly improve their data security, and provides independent, expert oversight of PCC's and QRS's security systems.

PARTIES

22. Plaintiff K.L. was a patient of PCC in Missouri when it collected and received her Protected Information that PCC then maintained in its database, email, computer systems, and other medical records systems. Her Protected Information was compromised in the Protected Information Security Failure. All of Plaintiff K.L.'s treatment and consultations with PCC occurred in Missouri. Plaintiff is a citizen of the State of Illinois.

23. Defendant PCC is an entity organized and existing under the laws of the State of Missouri. It has the capacity to be sued. PCC also does business throughout the state of Missouri.

24. PCC has four office locations, three in St. Louis County, Missouri and one in St. Charles County, Missouri. The vast majority of PCC's patients are Missourians. Indeed, upon information and belief, 70% or more of PCC's patients are Missourians, that is, citizens of Missouri.

25. Defendant QRS is a Tennessee corporation, is headquartered in Tennessee, and at all times material to this Complaint has been in good standing to transact business in the State of Tennessee.

26. QRS states on its website that its software "is used by providers to streamline their . . . data security, and more."

JURISDICTION AND VENUE

27. Plaintiff K.L. was first injured by conduct occurring, in part, in Tennessee. Plaintiff K.L. entrusted PCC with the Protected Information in Missouri. PCC, in turn, provided the

information to QRS. The third-party cybercriminals obtained the information from servers believed to be located in Tennessee.

28. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class are citizens of states that differ from the Defendants.

29. This Court has specific personal jurisdiction over Defendant PCC because PCC purposefully provided its patients' information to QRS in Tennessee. This controversy arises or relates to PCC's provision of its patients' information to QRS in Tennessee. It is not unfair for PCC to defend this case in Tennessee given its conduct and ongoing business relationship with QRS related to its patients' information.

30. This Court has both general and specific personal jurisdiction over Defendant QRS. QRS' principal place of business is in Tennessee and QRS is incorporated in Tennessee. As such, QRS is at home in Tennessee. Further, this controversy arises from the data security practices, omissions, and failures of QRS which occurred in Tennessee.

31. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Both defendants maintained Plaintiffs' information in this District, and have caused harm to Plaintiffs in this District.

32. Accordingly, this Court has jurisdiction over both the parties and the subject matter of this case.

FACTUAL ALLEGATIONS

33. PCC provides psychiatric and psychological medical care to its patients.

34. In providing medical care, PCC obtains patients' Protected Information. Indeed, PCC publishes a Notice of Privacy Practices in which it acknowledges its responsibility to protect patients' Protected Information.

35. All patients of PCC and its related entities are required to agree to the terms of a "Consent and Agreement." The parties to those contracts exchange mutual promises regarding PCC's provision of health care. Among the terms of that agreement is a specific incorporation of PCC's Notice of Privacy Practices.

36. Plaintiff K.L.'s Protected Information was compromised in the Protected Information Security Failure. Plaintiff K.L. spoke with an employee of PCC who informed her that the information compromised in the Protected Information Security Failure included treatment and diagnosis codes for treatment from at least 2018. These codes are standardized and can be quickly translated through a number of free online websites.

37. Plaintiff never waived the duty of confidentiality. Thus, PCC was not permitted to disclose Plaintiff's medical records and other Protected Information. There were also not any countervailing reasons for PCC to provide access to and disclose Plaintiff's medical records and other Protected Information.

38. PCC's Notice of Privacy Practices acknowledges PCC's duty to keep patients' Protected Information private.

39. PCC further had obligations created by HIPAA, industry standards, common law, and other representations made to Plaintiffs to keep Plaintiffs' Protected Information confidential and to protect Plaintiffs' Protected Information from unauthorized access and disclosure.

40. Plaintiffs provided their Protected Information to PCC with the reasonable expectation and mutual understanding that PCC and its business associates would comply with

their obligations to keep such information confidential and secure from unauthorized access and disclosure.

41. PCC's medical records security obligations were particularly important given the substantial increase in information security failures in the healthcare industry preceding the date of the Protected Information Security Failure. The increase in personal and medical information security failures—and the attendant risks of the same—was widely known to the public and to anyone in PCC's industry, including PCC.

42. PCC provided Plaintiffs' Protected Information to its vendor, QRS, to facilitate a patient portal that, among other things, allows for ease in processing payments and aids in collections. These patients' data was stored in QRS's systems that were compromised by the Protected Information Security Failure.

PCC Failed to Exercise Due Care in Contracting with QRS

43. PCC failed to exercise due care in protecting patients' information by contracting with QRS to handle its patient portal and or store PCC's medical record files.

44. PCC failed in its independent obligation to ensure that its HIPAA business associate employed reasonable and industry-standard data security measures.

45. Some of the easiest ways to minimize exposure to a data security incident are to limit the type and amount of information provided to business associates, and routine destruction or archiving of inactive PII and PHI so that it cannot not be accessed through online channels. The sheer number of records suggests that QRS was not destroying or archiving inactive records. Again, PCC would have discovered this had it exercised adequate oversight over its business associates and audited the data security protocols utilized by QRS.

46. PCC had an obligation to exercise oversight over QRS in a manner that would include immediate knowledge of any data security incident experienced by QRS that could affect PCC's patients.

47. According to QRS, it notified PCC of the Protected Information Security Failure within 10 days on September 7, 2021, and that additional information was shared with PCC on October 1, 2021. PCC, however, did not provide notice of the Protected Information Security Failure to its patients. Rather, PCC's patients had to hear about the failure from a vendor to whom they did not entrust their Protected Information. That notice did not come until November 26, 2021, *i.e.* 90 days after the Protected Information Security Failure was discovered.

48. The notice Plaintiffs received from QRS is deficient, not just because of its tardiness, but also because it does not detail any oversight taken by PCC over its business associates, nor is sufficient detail provided about how the Personal Information Security Failure occurred. Indeed, Plaintiff K.L. has never received any formal communication from PCC about the Personal Information Security Failure. Rather, the only information she has received has been through the letter she received from QRS and her own subsequent telephone inquiries.

Defendants' Protected Information Security Failure and
Defendants' Violations of HIPAA and Professional Standards

49. PCC agreed, and had a continuing contractual and common-law duty and obligation, to keep confidential the Protected Information its patients disclosed to it and to protect this information from unauthorized disclosure. PCC's agreements, duties, and obligations are based on: (1) HIPAA; (2) industry and professional standards; (3) the agreements and promises made to Plaintiffs; and (4) Section 5(a) of the FTCA, 15 U.S.C. § 45. Plaintiffs provided their Protected Information to PCC with the reasonable belief that PCC and its business associates

would comply with its agreements and any legal requirements to keep that Protected Information confidential and secure from unauthorized disclosure.

50. Like PCC, QRS agreed, and had a continuing contractual and common-law duty and obligation, to keep confidential the Protected Information disclosed to it and to protect this information from unauthorized disclosure. QRS's agreements, duties, and obligations are based on: (1) HIPAA; (2) industry and professional standards; (3) the agreements and promises made to Plaintiffs; and (4) Section 5(a) of the FTCA, 15 U.S.C. § 45. Plaintiffs provided their Protected Information to PCC and other healthcare providers with the reasonable belief that those healthcare providers and their business associates, like QRS here, would comply with their agreements and any legal requirements to keep that Protected Information confidential and secure from unauthorized disclosure.

51. HIPAA requires that PCC provide every patient it treats, including Plaintiffs, with a privacy notice. In this HIPAA-mandated privacy notice, PCC agrees that it will keep PHI of its patients, including Plaintiffs, confidential and protected from unauthorized disclosure.

52. PCC has a place for this Notice of Privacy Practices on its website, acknowledging its agreement, duty and promise to protect all PHI in its possession but that link has been disabled.¹ PCC also provides a HIPAA privacy notice to patients when they begin treatment.

53. PCC's data security agreements, obligations, and commitments are particularly important given the substantial increase in data breaches (particularly in the healthcare industry) during the period preceding the Protected Information Security Failure. PCC's failure to provide the data-security protections it committed to provide to Plaintiffs was particularly egregious in

¹ Patient Forms, <https://www.bhsmo.com/for-patients> [Privacy Practices] (last accessed Feb. 10, 2022).

light of specific government warnings regarding the possibility of attempts to illegally access the data of companies like PCC. Such warnings alerted PCC to the risk of a data breach and further emphasized PCC's duty to keep patients' Protected Information secure and to ensure that its business associates, such as QRS, kept its patients' Protected Information secure, as HIPAA mandates.

54. As alleged above, QRS was a "business associate" of PCC with whom PCC shared Protected Information of PCC's patients. Indeed, PCC was one of QRS's two largest clients. As PCC's business associate, QRS was required to maintain the privacy and security of Plaintiffs' Protected Information. HIPAA mandates that a covered entity (*i.e.* PCC) may only disclose PHI to a "business associate" (*i.e.* QRS) if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations. PCC failed to ensure that its business associate QRS safeguarded Protected Information of PCC's patients and that QRS complied with HIPAA's privacy mandates.

55. Both PCC and QRS had a non-delegable duty to ensure that all information they collected and stored was secure, and that any associated entities with whom they shared information maintained adequate and commercially-reasonable data security practices to ensure the protection of its patients' Protected Information.

56. HIPAA's Standards for Privacy of Individually Identifiable Health Information Security Standards for the Protection of Electronic Protected Health Information establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where

there is a “reasonable basis to believe the information can be used to identify the individual,” that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

57. HIPAA limits the permissible uses of “protected health information” and prohibits unauthorized disclosures of “protected health information.”

58. HIPAA requires that both PCC and QRS implement appropriate safeguards for this information.

59. HIPAA further mandates that a covered entity such as PCC may disclose PHI to a “business associate,” such as QRS, only if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.

60. HIPAA requires that PCC and QRS provide notice of a breach of unsecured PHI, which includes PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e.* non-encrypted data.

61. Beyond the regulatory requirements of HIPAA, PCC as a provider of psychological and psychiatric care should have also followed the record keeping guidelines of the American Psychological Association that have been in place since 2007 (“APA Guidelines”).² A number of

² *See Record Keeping Guidelines*, 62 Am. Psychologist 993 (Dec. 2007), <https://www.apa.org/practice/guidelines/record-keeping> (Dec. 2007) (last accessed Feb. 10, 2022).

those guidelines address PCC's duties to its patients to preserve patients' confidentiality related to mental health treatment, including, but not limited to, the following:

- a. Guideline 1—Responsibility for Records: Psychologists generally have responsibility for the maintenance and retention of their records;
- b. Guideline 3—Confidentiality of Records: The psychologist takes reasonable steps to establish and maintain the confidentiality of information arising from service delivery;
- c. Guideline 4—Disclosure of Record Keeping Procedures: When appropriate, psychologists inform clients of the nature and extent of record keeping procedures (including a statement on the limitations of confidentiality of the records; Ethics Code, Standard 4.02);
- d. Guideline 6—Security: The psychologist takes appropriate steps to protect records from unauthorized access, damage, and destruction; and
- e. Guideline 9—Electronic Records: Electronic records, like paper records, should be created and maintained in a way that is designed to protect their security, integrity, confidentiality, and appropriate access, as well as their compliance with applicable legal and ethical requirements.

62. Each of the APA Guidelines provides commentary including a prose rationale for the guideline and then a description of how the guideline applies in a real-world setting.

63. For instance, the rationale for Guideline 3 explains that, "The assurance of confidentiality is critical for the provision of many psychological services. Maintenance of confidentiality preserves the privacy of clients and promotes trust in the profession of psychology."³ As applied this guideline explains, "The psychologist maintains records in such a

³ *Id.* at 997.

way as to preserve their confidentiality. The psychologist develops procedures to protect the physical and electronic record from inadvertent or unauthorized disclosure.”⁴

64. The rationale for Guideline 6 reminded Defendant that, “Appropriate security procedures protect against the loss of or unauthorized access to the record, which could have serious consequences for both the client and psychologist.”⁵ And while Guideline 6 explains that off-site storage may be appropriate, such storage is subject to Guideline 9 which explains that electronic storage of client records poses special risks that require particular attention.⁶

65. Despite these requirements and professional guidance, both PCC and QRS failed to maintain their medical record systems in a manner that honored their duties and promises to Plaintiffs. PCC and QRS did not:

- a. adequately protect Plaintiffs’ Protected Information;
- b. properly monitor their medical records security systems, including those of their business associates, for unauthorized access or intrusions;
- c. maintain an adequate medical records security system to reduce the risk of medical records security failures and cyber-attacks;
- d. ensure that their business associates with access to their computer property employed reasonable medical records security procedures;
- e. ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1) and the APA Guidelines;

⁴ *Id.*

⁵ *Id.* at 998.

⁶ *Id.* at 1000.

- f. implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1) and the APA Guidelines;
- g. implement policies and procedures to prevent detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i) and the APA Guidelines;
- h. implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D) and the APA Guidelines;
- i. protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2) and the APA Guidelines;
- j. protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3) and the APA Guidelines;
- k. ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4) and the APA Guidelines; and/or
- l. train members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and the APA Guidelines.

66. Because of PCC's and QRS's failure to adequately apply security controls to their medical records systems, one or more cybercriminals were able to easily gain access to the

sensitive information of thousands of PCC patients and other patients whose information was stored by QRS—even though the individual(s) were not authorized to access such information.

Damages to Plaintiffs

67. Plaintiffs have been damaged by the compromise of their Protected Information.

68. Plaintiffs face risk of out-of-pocket fraud losses such as loans opened in their names, medical services building their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

69. Plaintiffs face increased risk of the publication and further compromise or theft of their Protected Information.

70. Plaintiffs face risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Protected Information—and in particular their PHI—because potential fraudsters could use that information to more effectively target such schemes to Plaintiffs.

71. Plaintiffs may also incur out-of-pocket and lost opportunity costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Protected Information Security Failure. Plaintiffs have lost time spent dealing with the Protected Information Security Failure.

72. Plaintiffs suffered a loss of value of their Protected Information when it was accessed and disclosed in the Protected Information Security Failure. Numerous courts have recognized the propriety of loss of value damages in medical records security failures and unauthorized medical information disclosure cases.

73. Plaintiffs were also damaged via benefit of the bargain damages. Such Plaintiffs overpaid for a service that was intended to be accompanied by adequate medical records security but was not. Part of the price Plaintiffs paid to PCC was intended to be used by PCC to fund

adequate security of PCC's computer property and Plaintiffs' Protected Information. Plaintiffs did not get what they paid for. Part of that price was to pay for QRS to provide adequate security for the information PCC provided to QRS. Thus, the actions, omissions, and failures of QRS detailed herein caused or contributed to cause Plaintiffs' contractual damages.

74. Plaintiffs now face the need to spend significant amounts of time to monitor their financial and medical accounts for misuse.

75. Plaintiffs have lost autonomy over their medical and treatment information and now have no idea who might have access to that information.

76. The U.S. Government Accountability Office noted in a report on data breaches (the "GAO Report") that identity thieves often use identifying data to open financial accounts, receive government benefits, and incur charges and credit in a person's name.⁷ As the GAO Report states, this type of identity theft is particularly harmful because it often takes time for the victim to become aware of the theft, and the theft can adversely impact the victim for years.

77. The GAO Report further states that victims of identity theft may face "substantial costs and inconveniences repairing damage to their credit records." *Id.* Identity theft victims are frequently required to spend significant amounts of time and money repairing the impact to their credit.

78. There may be a substantial time lag—measured in years—between when Protected Information is stolen and when it is used. According to the GAO Report: "[O]nce stolen data have been sold or posted to the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily

⁷ See U.S. Gov't Accountability Office, *Personal Information* (June 2007) <https://www.gao.gov/new.items/d07737.pdf> (last accessed Feb. 10, 2022)

rule out all future harm.” *Id.* Thus, Plaintiffs must vigilantly monitor their financial and medical accounts for many years to come.

79. With access to the type of information that was accessed in the Protected Information Security Failure, criminals can open accounts in victims’ names; receive medical service in the victims’ name; obtain a driver’s license or official identification card in the victim’s name but with the thief’s photo; use the victim’s name and Social Security Number to obtain government benefits; file a fraudulent tax return using the victim’s information; and give the victim’s personal information to police during an arrest, resulting in an arrest warrant being issued in the victim’s name.⁸

80. Protected Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often sell it on the cyber “black-market” or “dark web” indefinitely. Cyber criminals routinely post stolen Social Security Numbers, financial information, medical information, and other sensitive personal information on anonymous websites, making the information widely to a criminal underworld. There is an active and robust market for this information.

81. Medical information is especially valuable to identity thieves, and, accordingly, the medical industry has experienced disproportionately higher numbers of information theft events than other industries. PCC and QRS knew or should have known this and strengthened their information systems accordingly. PCC and QRS were put on notice of the substantial and foreseeable risk of harm from the Protected Information Security Failure, yet failed to properly prepare for that risk.

⁸ See Federal Trade Commission, Warning Signs of Identity Theft, <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last accessed Feb. 10, 2022).

82. Plaintiffs are at risk that the harms they have suffered will continue as their Protected Information that remains in PCC's and QRS's possession will continue to be at increased risk while PCC and QRS fail to undertake appropriate and adequate measures to safeguard Protected Information in their continued possession.

83. Plaintiffs have suffered loss of trust and confidence in health care providers and physicians.

84. PCC and QRS were, or should have been, aware that it was collecting highly valuable data, for which PCC and QRS knew, or should have known, there is an upward trend in data breaches in recent years. Accordingly, PCC and QRS were on notice for the harms that could ensue if it failed to protect Plaintiffs' data.

85. Protected Information is a valuable commodity to identity thieves. Compromised Protected Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers and other Protected Information directly on various dark web sites making the information publicly available.⁹

⁹ Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web* Experian (Dec. 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>; McFarland et al., *The Hidden Data Economy*, at 3, available at <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf> (last visited Feb. 10, 2022).

CLASS ACTION ALLEGATIONS

86. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23 (b)(2) and (b)(3) on behalf of two classes as defined as follows:

PCC Class

All patients of PCC whose Protected Information was compromised in the Protected Information Security Failure that was announced on or about November 26, 2021;

Illinois QRS Class

All persons residing in Illinois whose Protected Information was compromised in the Protected Information Security failure that was announced on or about November 26, 2021.

87. Excluded from the above class is the judge to whom this case is assigned and counsel.

88. The PCC Class and the Illinois Class are collectively referred to as the “Class” unless otherwise specified.

89. **Numerosity.** The class is so numerous that joinder of all members is impracticable. The class consists of thousands of individuals.

90. **Commonality.** There are many questions of law and/or fact common to Plaintiff K.L. and the Class. Common questions include, but are not limited to:

- a. Whether PCC’s and QRS’s medical records security systems prior to and during the Protected Information Security Failure complied with applicable medical records security laws and regulations including, *e.g.* HIPAA;
- b. Whether PCC’s and QRS’s medical records security systems prior to and during the Protected Information Security Failure were consistent with industry standards;

- c. Whether PCC and QRS owed a duty to Plaintiffs, to safeguard their Protected Information;
- d. Whether PCC and QRS breached their duty to Plaintiffs, to safeguard their Protected Information;
- e. Whether unauthorized bad actor(s) obtained Plaintiffs' Protected Information in the Protected Information Security Failure;
- f. Whether PCC and QRS provided sufficiently timely and substantively complete information to Plaintiffs about the Protected Information Security Failure; and
- g. Whether PCC and QRS knew or should have known that their medical records security systems and monitoring processes were deficient.

91. **Typicality.** Plaintiff K.L.'s claims are typical of the claims of the Class in that Plaintiff K.L., like all Class members, had her Protected Information compromised in the Protected Information Security Failure.

92. **Adequacy of Representation.** Plaintiff K.L. will fairly and adequately protect the interests of the Class. Plaintiff K.L. has retained competent and capable counsel with significant experience in complex class action litigation. Plaintiff K.L. and her counsel are committed to prosecuting this action vigorously on behalf of the Class. Plaintiff K.L.'s counsel has the financial and personnel resources to do so. Neither Plaintiff K.L. nor her counsel have interests that are contrary to, or that conflict with, those of the Class.

93. **Predominance.** PCC and QRS engaged in a common course of conduct toward Plaintiff and the Class. The common issues arising from PCC's and QRS's conduct affecting Plaintiffs predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

94. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Plaintiffs likely would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Plaintiffs would create a risk of inconsistent or varying adjudications with respect to individual Plaintiffs, which would establish incompatible standards of conduct for PCC and QRS. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each member of the Class. Indeed, PCC and QRS recognized this commonality when they sent the same basic form letters and notice to the approximately 11,187 consumers affected by the Protected Information Security Failure.

95. Additionally, PCC and QRS have acted on grounds that apply generally to the Class as a whole, so that injunctive relief is appropriate on a class-wide basis under Fed. R. Civ. P. 23(b)(2).

COUNT I
BREACH OF FIDUCIARY DUTY
(Against Defendant PCC only)

96. Plaintiffs re-allege and incorporate by reference the allegations of paragraphs 1–95 as if fully stated in this Count.

97. In light of the special relationship between PCC and Plaintiffs, because PCC was Plaintiffs' healthcare provider, whereby PCC became guardians of their Protected Information, PCC became a fiduciary created by its undertaking and guardianship of the Protected Information, to act primarily for the benefit of its patients, including Plaintiffs (1) for the safeguarding of

Plaintiffs' Protected Information; (2) to timely notify Plaintiffs of a medical records security failure and disclosure; and (3) to maintain complete and accurate records of what and where PCC's patients' Protected Information was and is stored.

98. PCC has a fiduciary duty to act for the benefit of Plaintiffs upon matters within the scope of its patients' relationship, in particular, to keep secure the Protected Information of its patients, including Plaintiffs.

99. PCC breached its fiduciary duties to Plaintiffs by failing to diligently investigate the Protected Information Security Failure to determine the number of Plaintiffs affected in a reasonable and practicable period of time.

100. PCC breached its fiduciary duties to Plaintiffs by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' Protected Information.

101. PCC breached its fiduciary duties owed to Plaintiffs by failing to timely notify and/or warn Plaintiffs of the Protected Information Security Failure.

102. PCC breached its fiduciary duties owed to Plaintiffs, by failing to ensure the confidentiality and integrity of electronic PHI that PCC created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

103. PCC breached its fiduciary duties owed to Plaintiffs by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

104. PCC breached its fiduciary duties owed to Plaintiffs by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1).

105. PCC breached its fiduciary duties owed to Plaintiffs by failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

106. PCC breached its fiduciary duties owed to Plaintiffs by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

107. PCC breached its fiduciary duties owed to Plaintiffs by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

108. PCC breached its fiduciary duties owed to Plaintiffs by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4).

109. PCC breached its fiduciary duties owed to Plaintiffs by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*

110. PCC breached its fiduciary duties owed to Plaintiffs by failing to effectively train and supervise all members of its workforce (including independent contractors) regarding its policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

111. PCC breached its fiduciary duties owed to Plaintiffs by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

112. PCC breached its fiduciary duties to Plaintiffs by otherwise failing to safeguard Plaintiffs' Protected Information.

113. As a direct and proximate result of PCC's breaches of its fiduciary duties, Plaintiffs have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses as described above.

COUNT II
NEGLIGENCE
(Against PCC and QRS)

114. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1–95 as if fully stated in this Count.

115. PCC required Plaintiffs, to submit non-public personal information to obtain medical services. PCC then shared this information with QRS for its own business purposes.

116. By collecting and storing this non-public personal information, and sharing it and using it for commercial gain, both PCC and QRS had a duty of care to use reasonable means to secure and safeguard their medical records systems—and Plaintiffs' Protected Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. PCC's and QRS's duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of an information security failure.

117. PCC and QRS each owed a duty of care to Plaintiffs to provide medical records security consistent with industry standards and other requirements discussed herein, and to ensure

that their systems and networks, and the personnel responsible for them, adequately protected the Protected Information.

118. PCC's and QRS's duty of care to use reasonable security measures arose as a result of the special relationship that existed between PCC and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Both PCC and QRS were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs from an information security failure.

119. PCC's and QRS's duty to use reasonable security measures under HIPAA required both PCC and QRS to "reasonably safeguard" confidential information from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes PHI within the meaning of HIPAA.

120. In addition, PCC and QRS had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair or deceptive acts or practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission, the unfair practice of failing to use reasonable measures to protect confidential information.

121. PCC's and QRS's duty to use reasonable care in protecting confidential information arose not only as a result of the statutes and regulations described above, but also because PCC and QRS are bound by industry standards to protect confidential Protected Information.

122. PCC and QRS breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs' Protected Information, and by failing to provide timely

notice of the Protected Information Security Failure. The specific negligent acts and omissions committed by PCC and QRS include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' Protected Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to adequately monitor their employees and agents;
- d. Allowing unauthorized access to Plaintiffs' Protected Information;
- e. Failing to detect in a timely manner that Plaintiffs' Protected Information had been compromised; and,
- f. Failing to timely notify Plaintiffs about the Protected Information Security Failure so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

123. It was foreseeable that PCC's and QRS's failure to use reasonable measures to protect Plaintiffs' Protected Information would result in injury to Plaintiffs. Further, the breach of security was reasonably foreseeable given the known high frequency of information security failure in the medical industry.

124. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' Protected Information would result in one or more types of injuries to Plaintiffs.

125. As a direct and proximate result of PCC's negligence, Plaintiffs have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses as described above.

COUNT III
NEGLIGENCE PER SE
(Against PCC and QRS)

126. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1–95 as if fully stated in this Count.

127. Pursuant to the FTCA (15 U.S.C. § 45), PCC and QRS had a duty to provide fair and adequate computer systems and information security practices to safeguard Plaintiffs’ Protected Information.

128. Pursuant to HIPAA (42 U.S.C. § 1320d, *et seq.*), PCC and QRS had a duty to implement reasonable safeguards to protect Plaintiffs’ Protected Information.

129. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) (“GLBA”), PCC and QRS had a duty to protect the security and confidentiality of Plaintiffs’ Protected Information.

130. PCC and QRS breached their duties to Plaintiffs, under the FTCA (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1320d *et seq.*), and the GLBA (15 U.S.C. § 6801) by failing to provide fair, reasonable, or adequate computer systems and information security practices to safeguard Plaintiffs’ Protected Information.

131. PCC’s and QRS’s failure to comply with applicable laws and regulations constitutes negligence per se.

132. But for PCC’s and QRS’s wrongful and negligent breach of their duties owed to Plaintiffs, Plaintiffs would not have been injured.

133. The injury and harm suffered by Plaintiffs was the reasonably foreseeable result of PCC’s and QRS’s breach of their duties. PCC and QRS knew or should have known that they were failing to meet their duties, and that PCC’s and QRS’s breach would cause Plaintiffs to experience the foreseeable harms associated with the exposure of their Protected Information.

134. As a direct and proximate result of PCC's and QRS's per se negligent conduct, Plaintiffs have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses as described above.

COUNT IV
BREACH OF CONTRACT
(Against PCC and QRS)

135. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1–95 as if fully stated in this Count.

136. When Plaintiffs provided their Protected Information to PCC in exchange for PCC's services, they entered into contracts with PCC pursuant to which PCC agreed to reasonably protect such information.

137. PCC solicited and invited Plaintiffs to provide their Protected Information as part of PCC's regular business practices. Plaintiffs accepted PCC's offers and provided their Protected Information to PCC.

138. In entering into such contracts, Plaintiffs reasonably believed and expected that PCC's information security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards. Further, Plaintiffs reasonably believed and expected that any vendors of PCC, like QRS would have information security practices that complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

139. Plaintiffs, who paid money to PCC, reasonably believed and expected that PCC and its vendors, like QRS here, would use part of those funds to obtain adequate information security. PCC and QRS failed to do so.

140. Plaintiffs would not have entrusted their Protected Information to PCC, and by extension, QRS, in the absence of the contract between them and PCC, and by extension QRS, to keep that information reasonably secure. Plaintiffs would not have entrusted its Protected Information to PCC or QRS in the absence of their implied promise to monitor PCC's and QRS's email and other systems to ensure that PCC and QRS adopted reasonable information security measures.

141. Plaintiffs fully and adequately performed their obligations under the contracts with PCC.

142. Plaintiffs were also the third-party beneficiaries of a contract between PCC and QRS whereby QRS promised to provide data protection services in maintaining Plaintiffs' Protected Information as its vendor and business associate.

143. PCC and QRS breached their contracts with Plaintiffs by failing to safeguard and protect Plaintiffs' Protected Information.

144. As a direct and proximate result of PCC's and QRS's breaches of contract, Plaintiffs have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses as described above.

COUNT V
MISSOURI MERCHANDISING PRACTICES ACT
MO. REV. STAT. § 407.101, *ET SEQ.*
(Against Defendant PCC only)

145. Plaintiffs re-allege and incorporate the allegations in paragraphs 1–95 as if fully stated in this Count.

146. PCC is a “person” as defined by the Missouri Merchandising Practices Act (“MMPA”), Mo. Rev. Stat. § 407.010(5).

147. Healthcare services are “merchandise” as defined by Mo. Rev. Stat. § 407.010(4).

148. Efforts to maintain the privacy and confidentiality of medical records are part of the healthcare services associated with a good.

149. Maintenance of medical records are “merchandise” within the meaning of the Mo. Rev. Stat. § 407.010(4).

150. PCC advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as those terms are defined in Mo. Rev. Stat. § 407.010.

151. Plaintiffs purchased or leased goods or services primarily for personal, family, or household purposes from PCC.

152. PCC engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020.1, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ Protected Information, which was a direct and proximate cause of the Protected Information Security Failure;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Protected Information Security Failure;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ Protected Information, including duties imposed by the FTCA, 15 U.S.C. § 45, the Fair Credit Reporting Act, 15 U.S.C. § 1681e (“FCRA”), and the

GLBA, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Protected Information Security Failure;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' Protected Information, including implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' Protected Information, including duties imposed by the FTCA, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' Protected Information, including duties imposed by the FTCA, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

153. PCC's conduct also violates the enabling regulations for the MMPA because it: (1) offends public policy; (2) is unethical, oppressive, and unscrupulous; (3) causes substantial injury to consumers; (4) is not in good faith; (5) is unconscionable; and (6) is unlawful. *See* Mo. Code Regs. Ann. tit. 15, § 60-8.

154. PCC's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of PCC's information security and ability to protect the confidentiality of consumers' Protected Information.

155. As a direct and proximate result of PCC's unlawful, unfair, and deceptive acts and practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from increased risk of fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Protected Information.

156. Plaintiffs seek all monetary and non-monetary relief allowed by law, including actual damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

COUNT VI
ILLINOIS CONSUMER FRAUD ACT
815 ILCS 505/1, *ET SEQ.*
(Against Defendant QRS only)

157. Plaintiffs re-allege and incorporate the allegations in paragraphs 1–95 as if fully stated in this Count.

158. At all times relevant hereto, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*, (hereinafter “ICFA”) prohibited “the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact ... in the conduct of any trade or commerce” and declared such acts or practices unlawful.

159. QRS's acts and omissions alleged in this Complaint occurred in commerce.

160. QRS represented to Plaintiffs that it had the capacity to protect Plaintiffs' Protected Information. This was false.

161. QRS represented to PCC and others that it would comply with state and federal law regarding protection of Plaintiffs' Protected Information. This was false.

162. QRS represented to PCC and others that it would protect Plaintiffs' Protected Information. This was false.

163. These representations were material to Plaintiffs' purchase of medical services from PCC in that PCC, as the agent of Plaintiffs, relied upon these representations in purchasing services from QRS.

164. QRS intended that PCC, and by extension, Plaintiffs, would rely on its deceptive, false, and misleading misrepresentations or omissions of material fact when entrusting their Protected Information to QRS.

165. But QRS failed to protect Plaintiffs' Protected Information. It failed to take the necessary steps to live up to the promises made to PCC, and by extension Plaintiffs.

166. QRS violated the ICFA by the use of deceptive, false, and misleading misrepresentations or omissions of material fact in connection with securing Plaintiffs' Protected Information. In particular, QRS lacked the capacity to protect Plaintiffs' Protected Information. QRS failed to comply with applicable state and federal law regarding protection of Plaintiffs' Protected Information. And QRS failed to adequately protect Plaintiffs' Protected Information.

167. As a direct and proximate result of QRS's failure to protect Plaintiffs' Protected Information, in violation of the ICFA, Plaintiffs' Protected Information that was entrusted to QRS was improperly accessed, copied, transferred, and/or disclosed.

168. As a direct and proximate result of Defendants' violations of the ICFA, Plaintiffs have been harmed, damaged, and/or injured as described above.

RELIEF REQUESTED

169. Plaintiffs request that the Court enter judgment against PCC and QRS, including the following:

- a. determining that this matter may proceed as a class action and certifying the Class asserted herein;
- b. appointing Plaintiff K.L. as representative of the Class and undersigned counsel as class counsel;
- c. an award to Plaintiffs of compensatory and consequential damages;
- d. injunctive relief requiring PCC and QRS to, *e.g.*: (i) strengthen their information security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring and identity theft protection to Plaintiff and the putative class members;
- e. an award requiring PCC and QRS to pay the cost of class notice;
- f. an award of attorneys' fees, costs, and expenses, as provided by law or equity;
- g. an award of pre-judgment and post-judgment interest, as provided by law or equity; and,
- h. such other or further relief as the Court may allow.

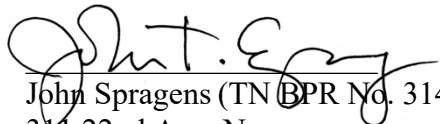
JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: February 16, 2022

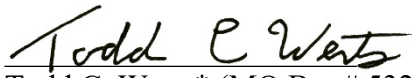
Respectfully submitted,

SPRAGENS LAW PLC



John Spragens (TN BPR No. 31445)
311 22nd Ave. N.
Nashville, TN 37203
T: (615) 983-8900
F: (615) 682-8533
john@spragenslaw.com

LEAR WERTS LLP



Todd C. Werts* (MO Bar # 53288)
103 Ripley Street
Columbia, Missouri 65201
Tel: 573-875-1991
Fax: 573-875-1985
Email: werts@learwerts.com

BUTSCH ROBERTS & ASSOCIATES, LLC

Christopher E. Roberts* (MO Bar # 61895)
231 S. Bemiston Ave., Ste. 260
Clayton, Missouri 63105
Tel: 314-863-5700
Email: croberts@butschroberts.com

Attorneys for Plaintiffs

**Pro Hac Vice Application Forthcoming*